

This document is an *example* of an **AI Office Policy** for purposes of establishing company guidelines for useage of AI software and platforms. For additional samples of *IT Security Polices* contact twald@riatatechnologies.com.

Definitions

Artificial Intelligence (AI):

Technology that simulates human intelligence to perform tasks such as reasoning, learning, planning, and problem-solving. Examples include ChatGPT, Claude, Microsoft Copilot, and Google Gemini.

AI System or Tool:

Any software, platform, or service that uses AI models to generate, analyze, predict, or automate tasks.

Generative AI (GenAI):

AI systems capable of creating original content such as text, images, or code based on user prompts.

Confidential Information:

Any company data, client data, or personally identifiable information (PII) that is not publicly available.

Public AI System:

AI services that process user data outside of company-controlled environments and may retain user prompts for model training (e.g., free or consumer versions of ChatGPT or Gemini).

Overview

This policy establishes guidelines for the responsible and ethical use of Artificial Intelligence (AI) technologies within <<COMPANY>>.

It is designed to safeguard <<COMPANY>>'s data, protect intellectual property, ensure compliance with applicable laws and regulations, and promote effective and secure use of AI tools in the workplace.

Purpose

The purpose of this policy is to define acceptable standards for using AI systems to support <<COMPANY>> operations. These standards are intended to minimize risks of data loss, privacy breaches, reputational harm, or unauthorized disclosure of confidential or client information.

Audience

This policy applies to all <<COMPANY>> employees, contractors, vendors, and authorized agents who access, utilize, or integrate AI technologies in the course of performing their duties on behalf of <<COMPANY>>.

Policy Detail

Acceptable Use

- AI tools may be used for research, drafting communications, summarizing data, automating workflows, and generating creative or analytical content.
- All AI-generated content must be reviewed by an authorized employee before being distributed externally.
- Employees must not input confidential, proprietary, or PII into any public AI systems.
- AI outputs are to be treated as drafts—they do not replace professional expertise or company-approved workflows.
- Any use of AI for decision-making that affects employees, clients, or business operations requires management review and approval.

Data Privacy and Security

- Sensitive or confidential data must never be entered into AI systems that store, retain, or train on user data.
- Only company-approved AI systems with enterprise-grade security may be used.
- All AI use must comply with <<COMPANY>>'s cybersecurity, data classification, and privacy policies.
- AI-generated content must not be used to collect, infer, or manipulate sensitive personal data without legal authorization.

Intellectual Property

- AI-generated materials created in the course of company business are the property of <<COMPANY>>.
- Employees must not use AI tools to infringe on any third-party copyrights, trademarks, or patents.
- Any external AI content incorporated into company materials must include proper attribution when applicable.

Accuracy and Accountability

- Users are responsible for validating the accuracy and appropriateness of all AI outputs.
- AI-generated recommendations, reports, or communications must be fact-checked and edited for compliance with <<COMPANY>>'s standards and values.
- Misuse or unverified reliance on AI-generated data is subject to disciplinary action.

Transparency

When AI tools are used to generate client-facing documents, marketing materials, or deliverables, employees must disclose AI assistance when legally required or ethically appropriate.

Training and Compliance

- <<COMPANY>> will provide ongoing training for responsible AI use.
- All users must complete annual training on AI ethics, security, and compliance.
- Violations of this policy may result in disciplinary action, up to and including termination.

Requirements

- Only IT-approved and licensed AI applications may be installed or accessed on company systems.
- Integration of AI systems into company workflows requires prior IT and management approval.
- Employees may not use personal AI accounts for company-related work.
- All AI-related incidents (e.g., data leakage, inaccurate output affecting business operations) must be reported to the IT Department immediately.

Review and Updates

This policy will be reviewed annually, or sooner as AI technologies evolve and regulatory standards change. Updates will be communicated to all employees and must be acknowledged electronically or in writing.

EXHIBIT A

Artificial Intelligence (AI) Office Policy Acknowledgement and Agreement

This Artificial Intelligence (AI) Office Policy Agreement ("Agreement") is entered into between the User and <<COMPANY NAME LEGAL>> ("<<COMPANY>>"), effective the date this agreement is executed by the User and <<COMPANY>>'s Information Technology Department ("IT"). The parties agree as follows:

ELIGIBILITY

Use of Artificial Intelligence (AI) systems and tools within <<COMPANY>> is a privilege granted to authorized employees, contractors, and agents under the AI Office Policy.

Failure to comply with the terms of this policy may result in suspension or revocation of access privileges, disciplinary action, or termination of employment or contract.

The purpose of this Agreement is to confirm the User's understanding and acceptance of <<COMPANY>>'s guidelines for ethical, secure, and compliant use of AI systems.

SECURITY CONSIDERATIONS AND ACCEPTABLE USE

- The User agrees to comply with all <<COMPANY>> policies related to data privacy, cybersecurity, acceptable use of information systems, confidentiality, and intellectual property.
- The User shall **not** enter any confidential, proprietary, client, or personally identifiable information (PII) into public or unapproved AI tools.
- AI tools are to be used only for legitimate business purposes and in accordance with the approved scope of duties assigned by <<COMPANY>>.
- All AI-generated content must be reviewed for accuracy, appropriateness, and compliance before being used or distributed.
- The User understands that AI systems may be monitored or audited for compliance purposes by the IT Department or authorized management.
- Unauthorized integration of AI tools into company workflows, systems, or client communications is strictly prohibited without prior IT and management approval.

ACCOUNTABILITY AND CONFIDENTIALITY

The User acknowledges that they are personally responsible for the accuracy, ethical use, and data integrity of all AI-assisted outputs they create or disseminate.

All intellectual property created using AI tools for company purposes remains the property of <<COMPANY>>.

The User agrees to immediately report any potential data breaches, AI misuse, or unauthorized disclosure of company information to IT or management.

TRAINING AND COMPLIANCE

The User agrees to complete any required AI awareness, security, and compliance training provided by <<COMPANY>> and to remain informed of policy updates or revisions.

Failure to complete mandatory training or comply with updates may result in suspension of AI system privileges.

ACKNOWLEDGEMENT

By signing this Agreement, the User certifies that they have read, understood, and agree to comply with all requirements of the **AI Office Policy**.

The User further understands that these obligations remain in effect even after termination of employment or engagement with <<COMPANY>>.

User

Date

HR Manager

Date